2016

National Security Agency & the 4th Amendment

James C. DeZao

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

Part of the Law Commons

Recommended Citation
https://scholarship.shu.edu/student_scholarship/765
NATIONAL SECURITY AGENCY & THE 4TH AMENDMENT

Current Topics in Internet Law
Professor Jennings
December 3, 2014

James C. DeZao
Since the birth of the United States of America in 1776, there has been a sense of secrecy that has been cast around particular branches of our government. From the Kennedy assassination to Watergate, there are many instances that make us question our government’s intentions, particularly those branches that are not entirely transparent.

The endless growth of technology in the world has only furthered our government’s agenda in keeping tabs on what is happening around the globe on a minute to minute basis. From the Middle East to the Mid-Western United States, the quest for information has been at its absolute highest level since September 11th, 2001.

Born in 1952, the National Security Agency has been on the forefront of this race to collect data. Having been given several nicknames and abbreviations, the NSA has also been dubbed “No Such Agency” based on its secretive nature. The NSA was formed by President Harry S. Truman to keep our country secure from foreign threats. The NSA was tasked to specialize in global monitoring, collection of data, decoding, translation and analysis of information, and counterintelligence that will
ultimately prevent attacks such as those on September 11th, 2001 and the Boston Marathon bombing.

Although the NSA has been tasked with the above mentioned items, there are a number of issues that have been brought to light within the past five years that have made the American Public question what the NSA is doing and whether or not it falls within the constraints of the United States Constitution.

On September 11th, 2001, the landscape of the world changed forever. There was no longer a sense of security that the American citizens once had knowing that an attack on American soil was highly unlikely. Along with the demeanor of the citizens, the landscape of the intelligence community as a whole took an entirely new turn, one that will change the course of its history forever. Six weeks post 9/11, current President, George W. Bush, signed the “Patriot Act” into effect which ultimately lowered protections against government intrusions.

“Surveillance of communications is another essential tool to pursue and stop terrorists. The existing law was written in the era of rotary telephones. This new law that I sign today will allow surveillance of all
communications used by terrorists, including e-mails, the Internet, and cell phones.\(^1\)” (Bush, 2001)

After the Patriot Act was put into place by President Bush, there were a number of actions that took place in the latter years that were questionable at best. In March of 2004, unknown to the public at the time, two senior government officials raced to the hospital in an attempt to make an end run at then Attorney General John Ashcroft to sign into effect an NSA wiretapping program that would allow them to bypass the need to obtain a warrant. This program would ultimately be uncovered over a year and a half later when the New York Times published an article detailing the policy.

“The previously undisclosed decision to permit some eavesdropping inside the country without court approval was a major shift in American intelligence-gathering practices, particularly for the National Security Agency, whose mission is to spy on communications abroad. As a result, some officials familiar with the continuing operation have questioned whether the surveillance has stretched, if not

crossed, constitutional limits on legal searches.\textsuperscript{2}

(LICHTBLAU, 2005)

This disclosure came as a shock to many Americans and became an often debatable topic of whether or not what the NSA was doing was in fact within the bounds of the United States Constitution. This collection of data is shown to be minute in comparison to what is eventually uncovered in a top secret intelligence program known as Prism.

On June 6\textsuperscript{th}, 2013, the intelligence world was turned upside down by a twenty nine year old, Booz Allen Hamilton contractor, named Edward Snowden. Snowden had begun one of the most controversial and revealing intelligence information leaks in the history of the United States. Among the classified documents that were leaked, there were a number of programs that had begun to make people question their government and its motives, particularly the National Security Agency. One of the most publicized and a controversial program disclosed was simply known as Prism.

From a detailed PowerPoint program leaked by Snowden, the Prism program was initially put into place in 2007 by the National Security Agency as an attempt to help monitor the activity of foreign intelligence overseas. However, this program

quickly shifted its target from those individuals overseas that may be deemed “terrorists” to domestic threats located within the bounds on the United States. Along with this shift, the Federal Government continued to bend the rules and hack the constitution to pieces in the eyes of many legal experts and citizens alike.

The concept of the Prism program is rather simple in concept. First, the government chooses the top tier of internet companies, particularly Google, Microsoft, Apple, Yahoo, Facebook, Youtube, Skype, AOL, and PalTalk and targets them for the program. Once a target provider has been established, the Prism Program will pull data directly from the servers of the target provider and compile it into the NSA database. All of this information will begin to make a mosaic of an individual’s life, habits, and tendencies.

Through the collection of meta-data, the NSA is able to compile such a mosaic of information and conclude what is or may be happening in your life at any given time.

Example: 1. You made a credit card purchase at a pharmacy 2. You search “Am I pregnant” via Google search engines 3. Shortly after, a phone call was placed to an OBGYN. Through this process, the
government is able to compile data and conclude that you are pregnant.

Upon the release of the PowerPoint slides, all of the above referenced providers adamantly denied that they had cooperated in any manner with the NSA and the mining of data from the servers. "Facebook is not and has never been part of any program to give the U.S. or any other government direct access to our servers." says Facebook founder and CEO Mark Zuckerberg. Similar statements have been released by almost every company involved in the program in the days after the leak was made. This should come as no surprise that companies that pride themselves on password protection and user anonymity would vehemently deny such involvement in a government spy program.

There are a number of people who do not believe that the internet giants have not cooperated with the Prism Program. In an exchange of emails between 2011 and 2012, Google chairman Eric Schmidt and NSA director Keith Alexander, had discussed multiple meetings that were to take place between Google executives and top government officials to discuss “Mobility threats and security”. These conversations took place long before the leak by Snowden in 2013 and demonstrate that Google

in particular may have been involved in the Prism program long before the American public ever heard of Edward Snowden. According to the slides released by Snowden, Google was brought on board with the Prism program in January of 2009.

A second program that has been put into practice by the NSA is similar to Prism however a different manner that the data is mined is being used. “Upstream” is similar to the Prism program in that it collects and compiles meta-data about an individual target. Upstream data mining is done by filtering out information as it passes through fiber optic cables used to transport the data.

In most instances, when information is transported over the World Wide Web from state to state or country to country, it is done so via fiber optic cables. These cables are typically small in size and relatively light weight. The advantage of using fiber optic cabling rather than satellites to move data from point A to point B can be seen in two important aspects, reliability and cost efficiency. There is a rather complex grid of cables that are laced around the world, under oceans, that connect every major country from the United States, the United Kingdom, France, Germany, Netherlands, etc. Surprisingly enough, the biggest threat to these cable networks are not the Sharks that have notoriously bitten them causing disruption of data.
flow, but the National Security Agency’s fingers poking through the Kevlar reinforced lines.

Despite being a clandestine foreign intelligence program, Upstream is able to capture an abundance of meta-data as it passes through the United States and cable networks located underneath oceans. As seen in the NSA slides released by Snowden, the abundance of communications in Europe, Asia & Pacific countries, and Latin America pass through the United States at one point prior to reaching their destination. The NSA has been able to exploit this streaming of data and use it to its advantage. Communications between people in foreign countries are able to be filtered out as they merely pass through the infrastructure used to connect the world. This is a “dragnet” approach to data collection. An abundance of data is collected as it passes by the fiber optic cables by a net that is placed between points A and B. This then allows the National Security Agency’s analysts like Edward Snowden to compile the data in such a fashion that you now have a profile which is stored and may or may not ever be used.

These two programs are typically used in conjunction with one another when they are implemented properly. The dragnet approach of Upstream does the initial meta-data collection. Once the bulk of the data has been collected, Prism is able to step
in and “fill the gaps” that are left after Upstream. One issue that is faced by Upstream data mining is that parts of the information that is sent over the internet is encrypted and cannot be viewed without proper keys or software to unencrypt said data. This is an obvious disadvantage to the Upstream program as an analyst cannot use what he cannot get. One way that the NSA is able to solve this problem is through Prism. Prism is able to step right into the servers of the provider and pick out what is needed to fulfill the targeting likely not hitting any encryption road blocks.

Once this enormous amount of data is mined from both Prism and Upstream, the material is only useful if it is able to be stored and accessed at a later date. The solution to this problem came in the form of a 1.5 billion-dollar, one million square foot building built in the middle of Utah. The National Security Agency’s “Utah Data Center” is among one of the largest if not the most advanced data centers located in the United States that we know about. The government felt it necessary to supply such a large asset with every amenity in order to keep the programs running at full capacity. The facility is said to use approximately 65 mega-watts of power according to Fox News. This is approximately enough to power 33,000 homes.
Once the public was initially made aware of these programs, the questions of legality followed soon thereafter. There are a few laws that these two programs rely on to operate in a “legal” way. The Foreign Intelligence Surveillance Act of 1978, FISA for short, is the platform that the programs operate under. Particularly, Section 702 of the FISA Amendments of 2008 allow both Prism and Upstream to operate freely. Section 702 does have a number of boundaries that the programs must stay within.

(b) Limitations

An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

50 U.S.C.A. § 1881a (West)
When evaluating the laws and acts that the National Security Agency relies upon to operate freely, one must fully understand who and what agencies or branches are putting these regulations in place. In this instance, the Foreign Intelligence Surveillance Court, FISC for short, has a very secretive and close door nature much like that of the NSA.

The FISC was born in 1978 when Congress also enacted the Foreign Intelligence Surveillance Act, FISA. The court is made up of eleven district court judges that are handpicked by the Chief Justice of the United States. The criteria for judges must be that they are picked from at least seven different judicial circuits and must serve a maximum of seven years. Furthermore there must be three judges that reside within 20 miles of Washington D.C., where the FISC is located to ensure speedy and timely response to warrant applications.

The main objective of the FISC is to grant “warrants” as the National Security Agency and its analysts see fit. To the naked eye, this process may lead a non-informed American Citizen to believe that the NSA and FISC are operating legally and in a transparent manner.

According to President Barack Obama and many senior government officials, the programs in place do not allow the NSA to listen into any of your private communications unless they
have gotten a warrant by the FISC. In a recent article published by The Washington Post, the number of warrants approved by the FISC is far higher than that of the regular judicial system. In the recent years since September 11th, 2001, the FISC warrant applications has jumped from a roughly 600 annually to a staggering 2,000+ per year. This increase would likely lead one to believe that the number of applications being denied has significantly increased given the rise in applications however that cannot be further from the truth. According to multiple media sources, since September 11th, 2001, there have only been 11 warrant applications that have been denied by the FISC. Additionally in some years post September 11th, there have been a perfect approval rating for warrant applications to the FISC.

Given the vast amount of applications that are approved by the FISC, it is reasonable to assume that there would not be any issue in obtaining an unjustified warrant against someone who has absolutely no ties with any terrorist organization. Additionally, the court is surrounded by secrecy and although records and transcripts are kept, they are not available to the public. If what the National Security Agency and the FISC is deemed legal and transparent by so many politicians and law makers, why the American public must be kept in the dark is a mystery.
Furthermore, in 2008, President Bush and Congress elected to revise surveillance laws to give the NSA even further reach into the homes of the American public. The main focus of the 2008 revision of the Foreign Intelligence Surveillance Act was to end the need for the FISC and essentially end the need for warrants to monitor the communications of people both domestic and abroad.

“The measure gives the executive branch broader latitude in eavesdropping on people abroad and at home who it believes are tied to terrorism, and it reduces the role of a secret intelligence court in overseeing some operations.” (ERIC LICHTBLAU, 2008)

In addition to these loosed restraints that the NSA and the government now had, they companies that had been complying with the programs were also now protected. One of the first major leaks to become public was that Verizon had been cooperating with the government and ultimately handing over vast amounts of information pertaining to phone call and data transmissions made by many if not all of their subscribers. The new amendments that were passed in 2008 now gave companies such as Verizon retroactive immunity against any lawsuits that may arise out of these disclosures.

---

“The measure, approved by a vote of 69 to 28, is the biggest revamping of federal surveillance law in 30 years. It includes a divisive element that Mr. Bush had deemed essential: legal immunity for the phone companies that cooperated in the National Security Agency wiretapping program he approved after the Sept. 11 attacks." (ERIC LICHTBLAU, 2008)

The revisions put in place in 2008 were a major stepping stone for the intelligence community and ultimately getting to the current state that they operate in. Immunity for the companies that cooperate in the programs, warrantless wiretaps and data mining, and very little if any oversight or transparency have laid the groundwork for a constitutional violation.

The first aspect that need be examined when addressing constitutionality is the most obvious, the 4th Amendment. The main focus of the 4th Amendment of the United States Constitution is to ensure that American citizens are protected against unjust and general government searches and seizures. Simplified, any government agency needs to have probable cause in order to obtain a warrant from the court to search your home, your vehicle, or your belongings.

—

The Prism and Upstream programs alike have been accused of violating Constitutional rights found under the 4th Amendment. There are two prongs that must be examined when addressing this issue. The first is where the data is being mined from. In most instances of data mining, both Prism and Upstream gather information from networks that are holding the information or grab it as it passes through optic cabling.

This is very similar to the transmission of your voice over copper lines when making a phone call to another individual. Historically, it has been deemed that these transmissions are private despite them moving over “public” channels of communication. As seen in Katz v. United States, the Supreme Court held that a warrantless wiretap of a public phone booth was in direct violation of Mr. Katz’ 4th Amendment right. Despite the fact that the government had reasonable suspicion that Mr. Katz was conducting illegal activities, they neglected to obtain a proper warrant. Though Mr. Katz knew he was committing a crime, he still was under the assumption that there is a reasonable amount of privacy given to him under the 4th Amendment thus protecting him against an unlawful search. Had the government made an application to the court with probable cause they would have likely been given a warrant and ultimately a conviction. However, the longstanding tradition of the
government looking to cut corners and violate Constitutional rights ultimately reared its ugly head.

The same concept can be argued in the collection of data from optic cables via the Upstream program. Users, regardless of whether or not they are committing a crime, are entitled to an assurance that they will not be subject to general or warrantless searches and seizures. Despite the fact that they information is being transmitted over “public” lines, they are still afforded the same amount of protection that is given to someone who is confined to the walls of their own home.

The second aspect of the 4th Amendment violation that may be occurring is the intrusion that is being committed by the Prism program. As previously discussed, the Prism program is a backdoor that is left open into the servers of just about every major internet service provider in order to allow the National Security Agency to pull information directly from the servers. This action must be carefully scrutinized as an ordinary citizen may deem this to be constitutional.

On its face, this practice may seem completely legal as the companies who ultimately store and transmit the data the NSA seeks is allowing them to enter into their servers. However, much like the practice of wiretapping, the fact that the provider allows the NSA and Prism program to feed off
information that it is holding “in trust” for its users shows the clear “general” search and seizure by the government. In both of the means that Upstream and Prism use to collect data, it is likely that many courts would construe this as a search within the 4th Amendment. The opinion in Katz unequivocally states that there must be a warrant for electronic wiretapping. I see no clear delineation between what the government was doing in Katz and what the NSA is doing with Prism and Upstream. It is a warrantless “tapping” of our infrastructure and a clear violation of our Constitutional rights.

As seen in Klayman v. Obama, Plaintiff Larry Klayman challenged the practice of meta-data collection by the NSA and ultimately prevailed in a preliminary injunction ruling. The very important question of whether or not the collection of such data is considered a search under the constitutional definition was answered by U.S. District Court Judge Richard Leon.

“Rather, the question that I will ultimately have to answer when I reach the merits of this case someday is whether people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to
high-tech querying and analysis without any case-by-case judicial approval. For the many reasons set forth above, it is significantly likely that on that day, I will answer that question in plaintiffs' favor.”


Assuming that the searches and ultimately seizures occurring within the Prism and Upstream program do constitute a violation of the 4th Amendment, there are many arguments that are made in support of such violations. The most obvious of all of the arguments is that these policies and procedures are for the greater good of the United States citizens as a whole.

Historically, there has been a debate as to whether violating the rights of one individual to benefit the group is morally and ethically correct. With regard to the United States Constitution, that debate is taken a step further and goes as far as examining the rights given to an individual by the architects of our government.

After the NSA information leaks by Edward Snowden in 2013, there was a great outcry by the American Public with regard to the programs. President Barack Obama took to the podium and attempted to address some of these concerns. In an alarming, yet
candid speech, the President told Americans that it was difficult to have complete security and complete privacy. This seems to almost admit that there is a constitutional violation occurring however the fact that it is benefitting the security of the United States it should be overlooked.

The 4th Amendment is put into place to ensure that American citizens are afforded complete security as well as complete privacy. There is no evidence to suggest that drafters or the legislature intended for the 4th Amendment to have a provision that states, “So long as the government feels fit, they may violate this clause at will”. Professor Johnathan Hafetz of Seton Hall Law School describes in a recent article the purpose of judicial review and 4th Amendment protections.

“The Fourth Amendment provides a bulwark against this type of dragnet surveillance. Before searching Americans’ private communications, the Fourth Amendment requires that the government demonstrate probable cause or individualized suspicion.” (Hafetz, 2013)

In many, if not all, instances of dragnet surveillance, the government has failed to demonstrate probable cause or individualized suspicion.

---

The justification of a clear constitutional violation in the name of national security shows that not only does the NSA know that what it is doing is wrong, but they are rewarded for doing so. Conversely, there are many aspects and practices that the government implements that are not deemed “legal”.

Enhanced interrogation, torture, was widely used in the post September 11th era as a necessary evil. Many tactics used have now been outlawed with the President and lawmakers alike speaking out against such practices. It is argued that torture is a violation of primarily the 8th Amendment of the Constitution that specifically protects individuals against “cruel and unusual punishment”. Torture, or enhanced interrogation as the government likes to call it, is often times used as a form of “punishment” if one is not cooperating with authorities during an interrogation.

While the majority of government officials do not condone the use of torture in order to gain information, one can argue that the use of such techniques is beneficial for the American public as a whole. It can be deemed similar that when the 4th Amendment rights of an individual must be violated in order to protect the vast majority of the American public, torture should also be seen as a necessary evil in order to protect the American public. While on one hand the government justifies
pushing 4\textsuperscript{th} Amendment rights to the side it also uses the same basis to disallow the use of torture as an interrogation method.

The Prism program and Upstream program alike feed off of the information that is being sent between two individuals or groups. More importantly, there are a number of rights that may be infringed upon in a less direct manner than that of the 4\textsuperscript{th} Amendment right to warrantless searches and seizures.

The 1\textsuperscript{st} Amendment affords the American citizens the freedom of speech and freedom of expression. This idea is was put into place in order to allow the creative and free flow of ideas between parties. This has been demonstrated in many Supreme Court decisions when addressing 1\textsuperscript{st} Amendment rights. Chief Justice Rehnquist elaborates in Hustler Magazine v. Falwell:


The intrusion by the government into the private conversations of Americans will eventually, if it hasn’t already, begin to impede the flow of ideas between creators, lawyers, doctors, and artist alike. If a law abiding citizen is
not protected from the government's surveillance as it brushes aside the Constitution, it is reasonable to believe that an attorney, working on a high profile criminal matter, would not feel comfortable communicating with his/her client through public lines of communication in fear that the prosecution may "inadvertently" filter out their conversation and use it to their advantage.

After the leaks by Edward Snowden, he was asked what his biggest fear was. It was not that he would be prosecuted and convicted of treason, it was not fear of imprisonment, it was a fear that nothing would change. The reach and power of the Federal Government is unmeasurable in today's day and age. Though the NSA has violated Constitutional Rights thousands, if not hundreds of thousands of times, each year, the biggest issue may lead to "targeting" of an individual that has absolutely no ties with a criminal organization at all. Snowden goes on to state that,

"Even if you’re not doing anything wrong, you’re being watched and recorded. ...it’s getting to the point where you don’t have to have done anything wrong, you simply have to eventually fall under suspicion from somebody, even by a wrong call, and then they can use this system to go back in time and scrutinize every
decision you’ve ever made, every friend you’ve ever discussed something with, and attack you on that basis, to sort of derive suspicion from an innocent life.”

Clear lines of delineation between lawful surveillance and government intrusion must be drawn in order to preserve the safety of every American now and in the future as technology progresses.

The system of checks and balances has been put into place in order to protect citizens against being kept ruled by a single individual. If the government and the National Security Agency alike are able to have absolute power over how and when they can target any individual person in the world, they are being handed the ability to convict people based on mere decision rather than a factual basis. Due process was put into place for a reason and must be preserved.

There has been a number of recent lawsuits filed and ultimately litigated pertaining to the National Security Agency and its practices. One notable case was brought by the American Civil Liberties Union (ACLU) against James R. Clapper, the current Director of National Intelligence.

---

ACLU v. Clapper was brought to challenge the constitutionality of the National Security Agency’s mass surveillance practices, notably Prism and Upstream programs. The basis of the suit was set into motion by revelations by “The Guardian” when they released an order from the FISC showing that Verizon Business Network Services was being forced to turn over records of their customers to the NSA. The ACLU was a customer at the time that these collections were occurring and more than likely had their information filtered.

Upon presentation of the court, a federal court judge denied the ACLU request for preliminary injunction and granted the NSA’s motion for dismissal. ACLU appealed to the Second Circuit Court of Appeals in Manhattan and is currently awaiting a decision on their appeal.

One of the biggest issues seen in recent litigation against the NSA and its programs is standing. Clapper v. Amnesty International may prevent many of these cases from ever making it past a simple Rule 12 motion.

In Clapper, the Supreme Court dismissed the suit for lack of standing. Furthermore, Justice Alito, said that the suit was based on a “highly speculative fear” that the government has been or will target their communications of the parties involved or any American Citizen for that matter. The court goes on to
stress that most of the claims put forth in the complaint are merely speculative with no substantiation or damages.

While I think that the fact that standing has not demonstrated is damaging, it is a Catch-22. In one instance, the complaint is not likely to make it past the initial pleadings as the plaintiff is unable to show that their communications have been filtered out. Conversely, they cannot demonstrate this unless they reach discovery, however most, if not all, of the programs are highly classified with no information readily available. Justice Alito goes on to state in his summation,

“We hold that respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm.” Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1155, 185 L. Ed. 2d 264 (2013)

Although the initial complaint did not make it beyond the initial pleadings, landmark cases such as this, Klayman, and others to come in the near future are the first step in securing the Constitutional rights of each American.

Moving forward, it is pressing that there is further litigation against the programs that the National Security
Agency has put into place in order to keep tabs on every communication that we have as law abiding citizens. The continued 4th Amendment violations that occur thousands of times per day are slowly but surely diminishing the boundaries that the Constitution has put into place to ensure that the United States does not fall under the rule of a dictator.

The government will continuously stand behind the argument that what they are doing is not only within constitutional constraints but that it is for the benefit of the country. While I do not believe that our founding fathers could have ever imagined the global community that we now live in would ever exist, we must still adhere to the fundamentals that they put into place. It is argued that the Constitution is outdated in comparison to our world, however that does not give the government free reign to disregard it in the interest of national security. If the Constitution is to be changed it must be done through proper legislation rather than secretive programs and back door dealings.

Edward Snowden, a Patriot, summed up the dealings rather appropriately in a recent interview. “The government has granted itself power it is not entitled to. There is no public
oversight. The result is people like myself have the latitude to go further than they are allowed to.⁸"

As this document is uploaded to the cloud and sent via email to its final destination, it is likely to be intercepted and analyzed. From this point forward, my communications, both past and future, are likely to be compiled and stored in a secret file, within a secret program, in a secret facility located somewhere in the middle of Utah. Could this be the first step in classifying me, a Patriot and law student, as a traitor? A terrorist? This unprecedented question will continue to erode our Constitutional Rights until we and our representatives take a stand to make change.

---